Assurance Cases

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Charles B. Weinstock
January 26, 2015

	Form Approved
# Report Documentation Page	OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **26 JAN 2015**	2. REPORT TYPE **N/A**	3. DATES COVERED	
4. TITLE AND SUBTITLE **Assurance Cases**		5a. CONTRACT NUMBER	
		5b. GRANT NUMBER	
		5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S) **Weinstock /Chuck**		5d. PROJECT NUMBER	
		5e. TASK NUMBER	
		5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213**		8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)		10. SPONSOR/MONITOR'S ACRONYM(S)	
		11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT **Approved for public release, distribution unlimited.**			
13. SUPPLEMENTARY NOTES **The original document contains color images.**			
14. ABSTRACT			
15. SUBJECT TERMS			

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT **SAR**	18. NUMBER OF PAGES **19**	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**			

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

Overview

Maturity of Assurance Cases

ISO 15026-2 Assurance Case Standard

Goal Structured Notation

Example from Industry

Confidence Work at the SEI

Other Current Work on Assurance Cases

Closing Thoughts

Maturity of Assurance Case Technology

Developed in late 90s in Europe

Used for safety cases in Europe for over 20 years

The UK Ministry of Defence *requires* generation of a compelling case to support claims that specific safety requirements are met:

> "The safety case shall consist of a **structured argument**, supported by a **body of evidence**, that provides a compelling, comprehensible and valid case that a **system is safe** for a given application in a given operating environment." [DEFSTAN 00-56 (Part 1)/4]

ISO standard under development (ISO 15026-2)

NRC Report: "Software for Dependable Systems: Sufficient Evidence?"

ISO/IEC 15026-2: Assurance Case
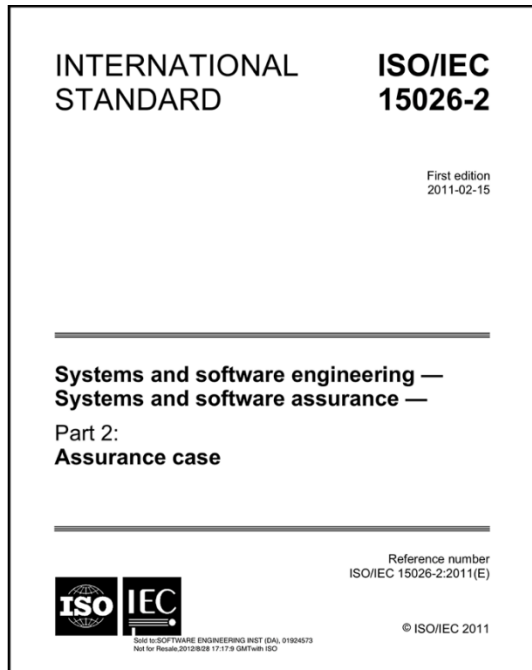
The assurance case is to be delivered and maintained with the system

Claim: A proposition to be assured (e.g., "The system is safe")

Evidence: A fact, datum, object, claim, or other assurance case

Argument: A reason why the set of evidence shows that the claim is true

Justification: A reason why a claim has been chosen

Assumption: A claim that appears as evidence

An *Assurance Case* is a quadruple a=(c,j,es,g) where c is a claim, j is a justification, es is a set of evidence, and g is an argument which assures c using es.
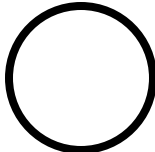
This definition is recursive
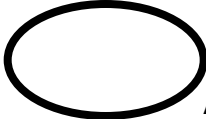
Goal Structuring Notation (GSN) – Kelly 1998

A specific notation for an assurance case consistent with 15026-2.

Developed to help organize and structure safety cases in a readily reviewable form

Used successfully for over a decade to document safety cases for aircraft avionics, rail signaling, air traffic control, and nuclear reactor shutdown

Shows how **claims** [ ] are broken down into sub-claims,

and eventually supported by **evidence** ◯ or [ ]

while making clear the argumentation **strategies** ▱ adopted,

the rationale for the approach (**assumptions, justifications**) ⬭ **A/J**

and the **context** ⬭ in which claims are stated

Example: Battery Exhaustion – Part One

Example: Battery Exhaustion – Part Two

C2

The battery exhaustion hazard has been adequately mitigated

C3

Caregiver is notified sufficiently soon (but not too soon) prior to battery exhaustion

Cx3

A late warning won't give the caregiver time to stop current activities and plug the pump in. An early warning may be ignored. This depends on the clinical setting.

C4

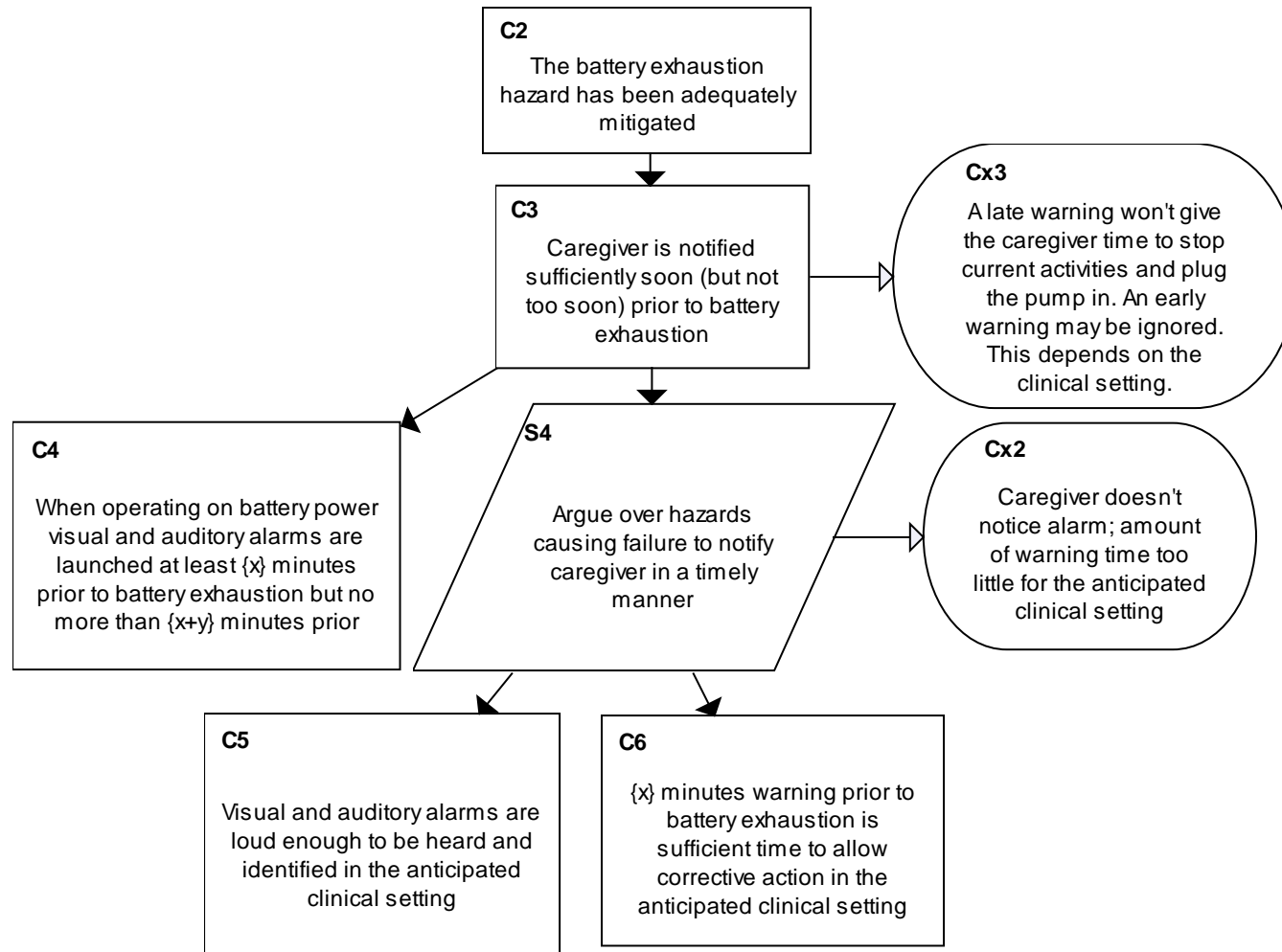When operating on battery power visual and auditory alarms are launched at least $\{x\}$ minutes prior to battery exhaustion but no more than $\{x+y\}$ minutes prior

S4

Argue over hazards causing failure to notify caregiver in a timely manner

Cx2

Caregiver doesn't notice alarm; amount of warning time too little for the anticipated clinical setting

C5

Visual and auditory alarms are loud enough to be heard and identified in the anticipated clinical setting

C6

$\{x\}$ minutes warning prior to battery exhaustion is sufficient time to allow corrective action in the anticipated clinical setting
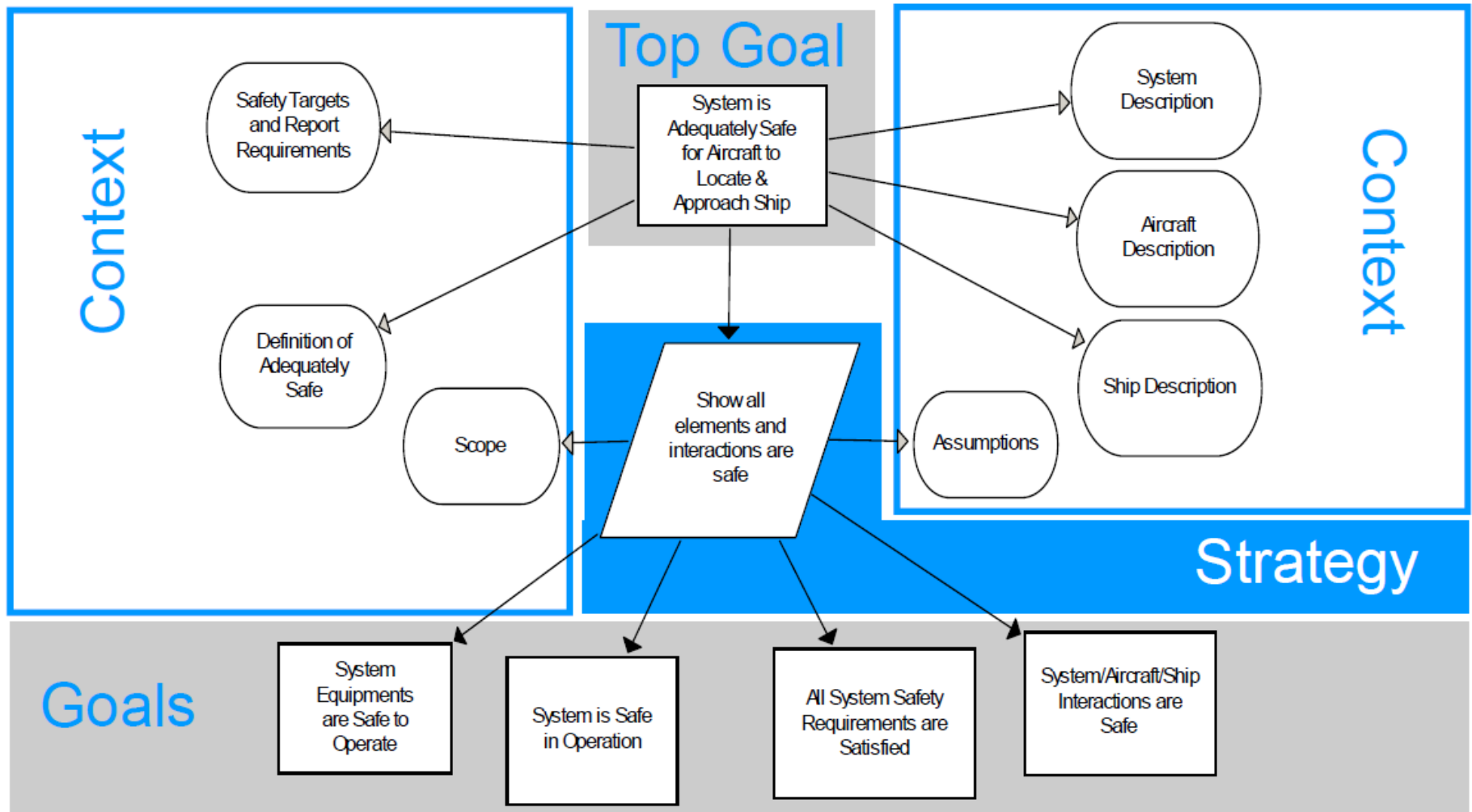
02 The Task

We were asked to assure the safety of a system for guiding aircraft onto ships in bad weather. This was to consider the whole ship/equipment/aircraft system of systems, taking into account:

- Human factors.

- The operating environment.

- Operating procedures.

- Maintenance & Management.

An Operational Safety Case (OSC) was needed.

05 Approach - OSC Safety Strategy

Top Goal

Context (left)
- Safety Targets and Report Requirements
- Definition of Adequately Safe
- Scope

Top Goal: System is Adequately Safe for Aircraft to Locate & Approach Ship

Context (right)
- System Description
- Aircraft Description
- Ship Description
- Assumptions

Strategy: Show all elements and interactions are safe

Goals
- System Equipments are Safe to Operate
- System is Safe in Operation
- All System Safety Requirements are Satisfied
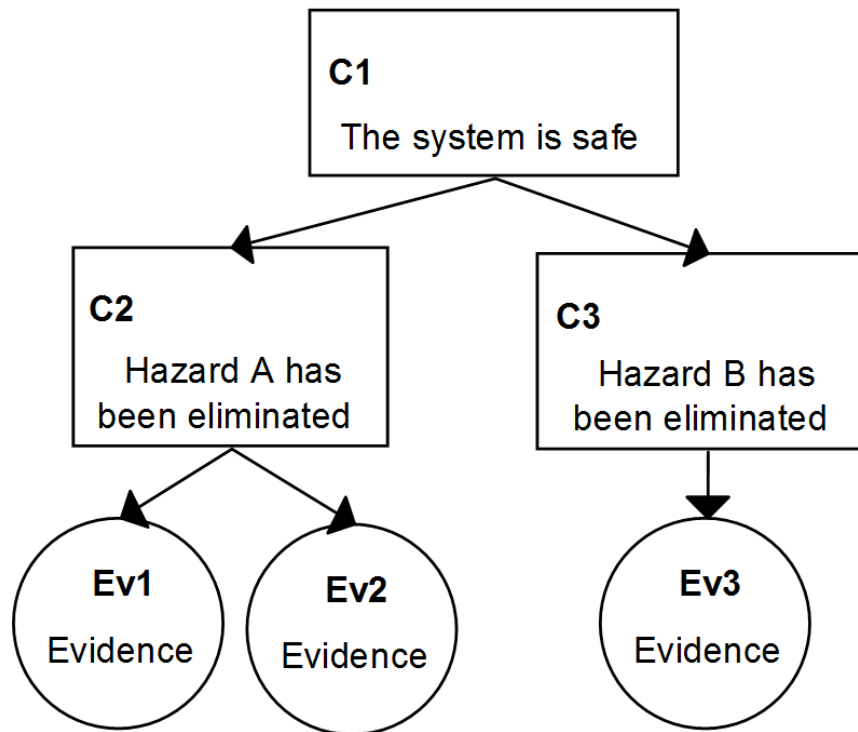- System/Aircraft/Ship Interactions are Safe

What confidence should be placed on an AC?

Given the evidence, how confident should we be in the claim C1? Why?

What does it mean to have confidence in the claim?

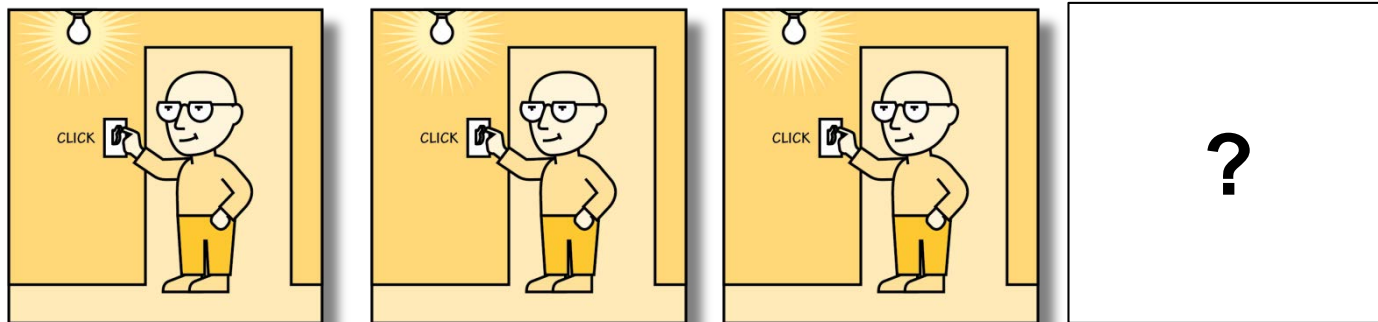What could be done to improve confidence? Why?

The Basis for Confidence in a Claim

A classic philosophical problem:

- Justify belief in a hypothesis

Use Induction

- **Enumerative**: Support increases as **confirming instances** are found
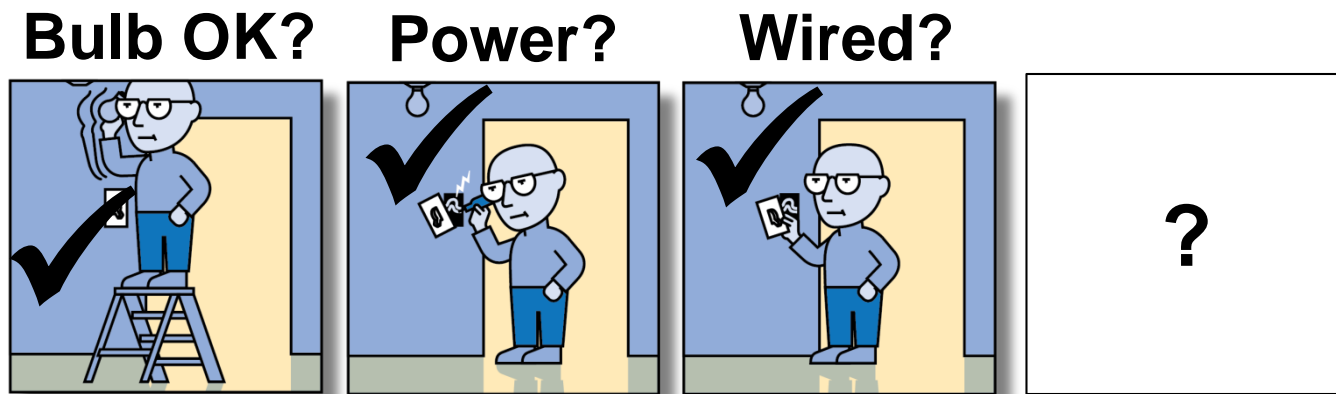

Using past experience as the basis for predicting future behavior

Eliminative Induction

Support for a claim increases as **reasons for doubt** are eliminated

CLAIM: The light turns on (when the switch is flicked).

Bulb OK? **Power?** **Wired?** **?**

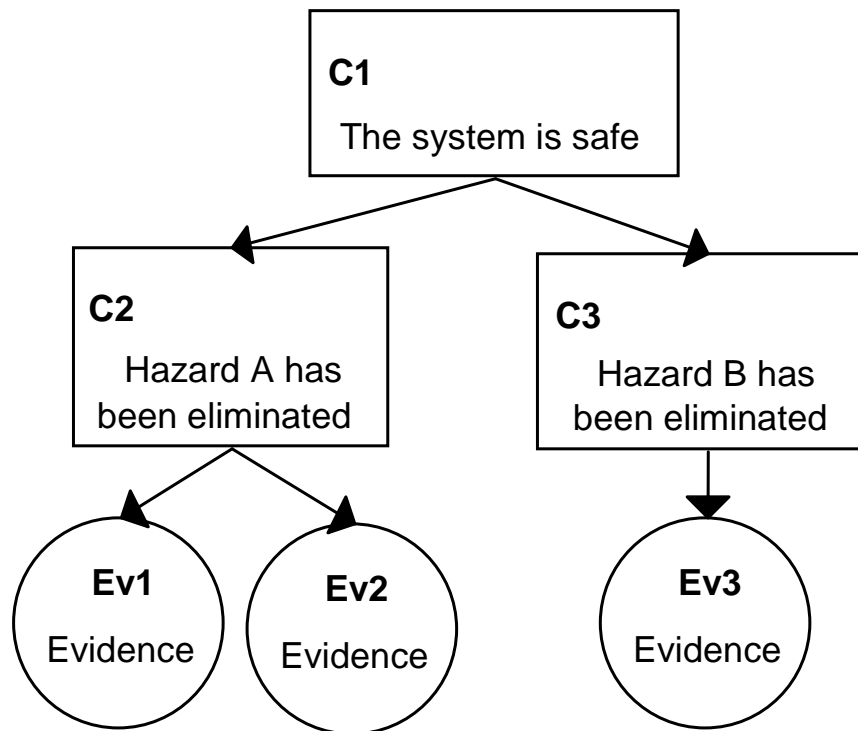**Confidence increases as doubts are eliminated**
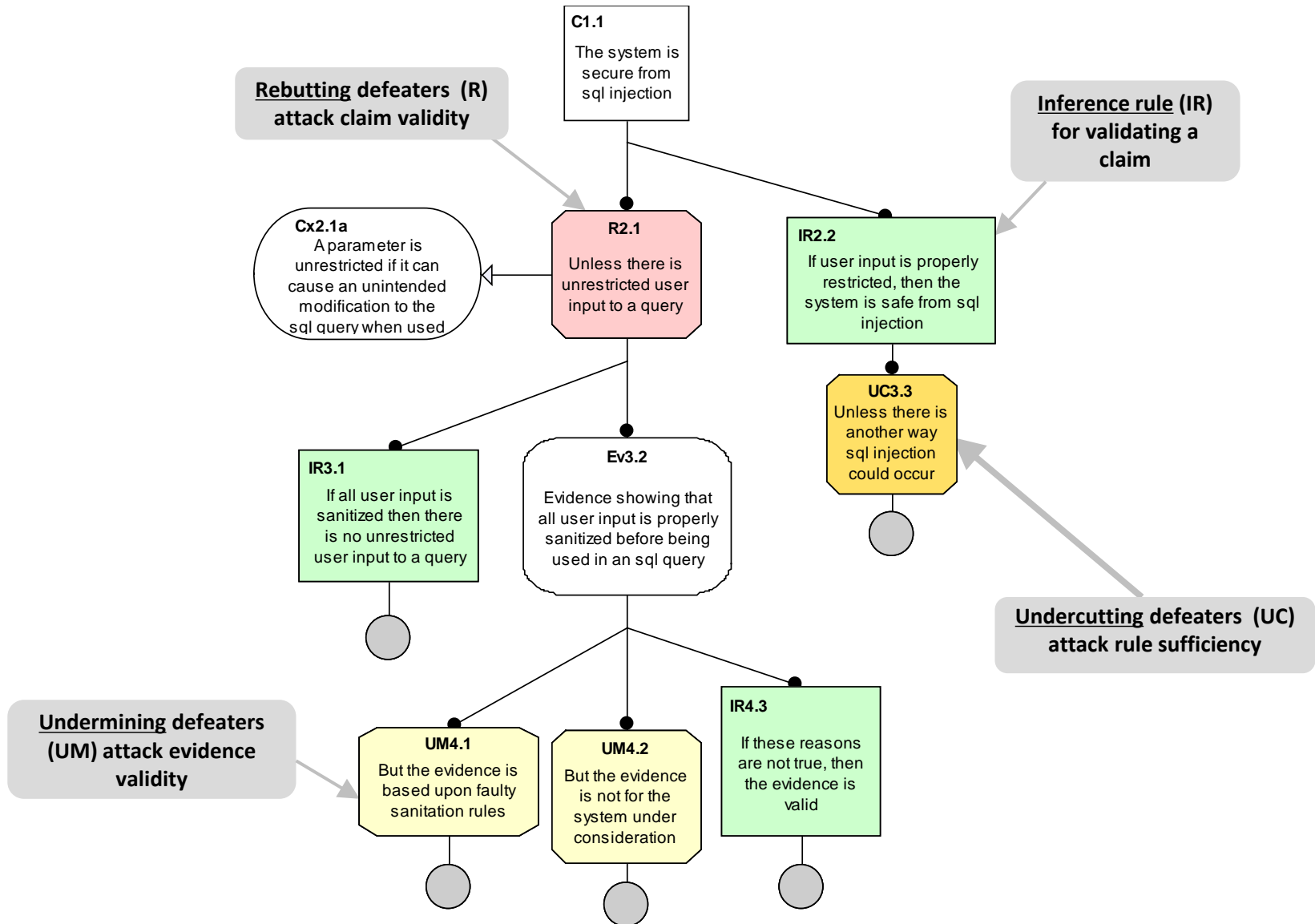
What confidence should be placed on an AC?

How confident in C1? Why? (Number of uneliminated doubts)

What does it mean to have confidence? (Lack of doubt)

What could be done to improve confidence? Why? (Elim. more doubts)

A Small Example

Key Ideas

Confidence grows as doubts are identified and eliminated

- Doubts about a claim (<u>rebutting</u> defeater)
  - Why claim may be **invalid**

> **R2.1**
>
> Unless there is unrestricted user input to a query

- Doubts about evidence (<u>undermining</u> defeater)
  - Why evidence may be **invalid**

> **UM4.1**
>
> But the evidence is based upon faulty sanitation rules

- Doubts about reasoning (<u>undercutting</u> defeater)
  - Premise ok; **conclusion uncertain**
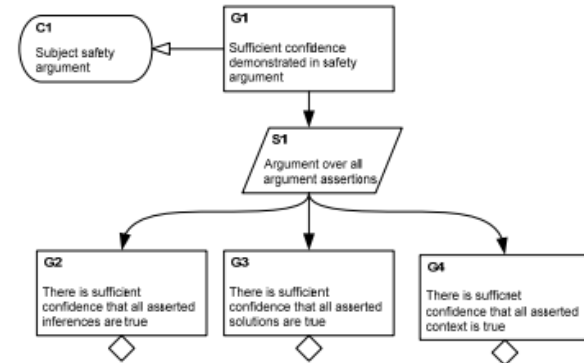
> **UC3.3**
> Unless there is another way sql injection could occur

Other State of the Art

John Knight – University of Virginia

- Confidence cases: a confidence argument created in parallel to the safety argument that documents the confidence in the structure and basis of the safety argument.

Tim Kelly – University of York

- Evidence elaboration: modeling evidence to better understand it and its evaluation for the purpose of explicit integration of the source data of evidence and the safety case argument.
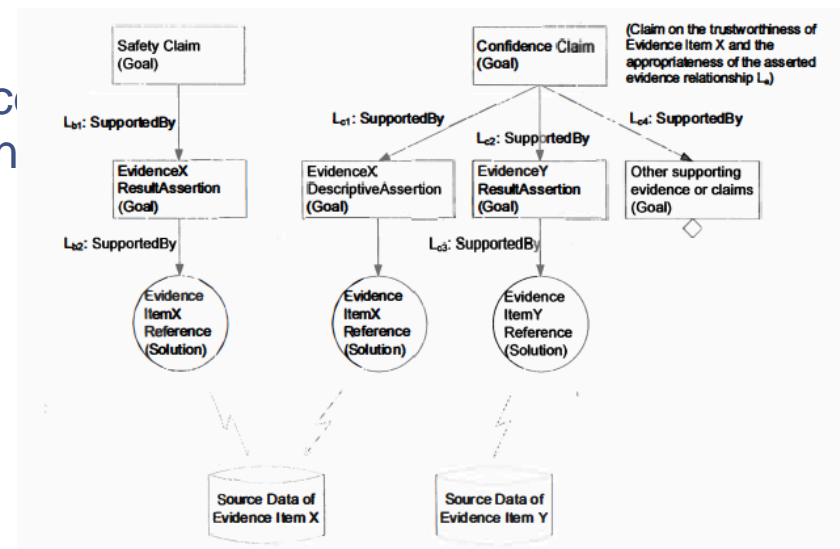
Concluding Thoughts

This has been a quick overview of assurance cases and confidence and an introduction to the concept eliminative argumentation as developed by the SEI.

- It is not a comprehensive review of all that is happening in the area.
- The SEI has been applying Baconian probabilities to confidence maps to show how much different portions of the argument contribute to overall confidence – something that may prove useful for incremental certification.

Assurance cases have been proven effective in the safety domain.

- The effectiveness of confidence cases and eliminative induction have yet to be demonstrated in practice.

Contact Information

Charles B. Weinstock

Principal Researcher

Software Solutions Division

Telephone: +1 412-268-7719

Email: weinstock@sei.cmu.edu

U.S. Mail

Software Engineering Institute

4500 Fifth Avenue

Pittsburgh, PA 15213-2612

USA